JSOC Security flash report Q3 2016

Отчет **Solar JSOC Security flash report** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за третий квартал 2016 года. В документе отражена сводная информация о выявленных инцидентах по различным категориям, отвечающая на вопрос о том, кто, как, в какое время и с использованием каких векторов и каналов реализовывал угрозы ИБ.

Отчет предназначен для информирования служб ИТ и информационной безопасности о текущем ландшафте угроз и основных трендах.

Оглавление

[1]ссылка - http://solarsecurity.ru/products/jsoc

info@solarsecurity.ru
+7 (499) 755-0770

Ключевые выводы

I

Статистика внешних инцидентов в Q3 2016 говорит об упрощении векторов преодоления периметров компаний и стремлении внешних злоумышленников к эксплуатации известных уязвимостей подсистем аутентификации и авторизации систем и сервисов.

II

В Q3 2016 было зарегистрировано 765 случаев компрометации административных учетных записей среди подключенных компаний-клиентов и порядка 1300 инцидентов, связанных с нарушениями использования управляющих протоколов систем и сервисов.

III

На длительном периоде времени замечено, что в компаниях, где используется SOC, наблюдается отсутствие роста, а иногда и снижение числа внутренних инцидентов. Это связанно с тем, что в компаниях-клиентах SOC гигиена ИБ повышается.

IV

На длительном периоде времени мы видим, что в третьем и четвёртом квартале растет доля внутренних инцидентов. Прежде всего это утечки конфиденциальных данных, заражение вирусами и компрометация внутренних учетных записей.

V

Продолжается уверенный рост числа утечек через почту. Несмотря на то, что этот канал обычно контролируется, сотрудники все равно используют его для нелегитимной передачи данных. Также это свидетельствует о том, что процесс обучения ИБ и Security awareness пока находится на недостаточно высоком уровне.

VI

В третьем квартале мы перестали фиксировать атаки на АРМ КБР. Это связано с усилиями ЦБ РФ по информированию банков о данном типе атак.

VII

Мы продолжаем отмечать, что внешние атаки смещаются ко времени, когда спадает деловая активность: 40% вечер пятницы/20% выходные/20% вечер.

VIII

Веб-приложения остаются одной из главных целей атак, но при этом меняется их источник – мы фиксируем все большее число попыток атак изнутри компании. Показательно распределение временных периодов атак: 70% день/10% вечер/20% ночь.

IX

Информационные бюллетени FinCERT позволили выявить 23 подтвержденных инцидента, из которых в 7 случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от атаки.

info@solarsecurity.ru
+7 (499) 755-0770

Общие положения

«Статистика угроз» является сводным материалом и результатом анализа инцидентов, выявленных командой Solar JSOC как в рамках оказания регулярных услуг мониторинга и реагирования на инциденты, так и консультативно-аналитической поддержки компаний российского рынка. Деление инцидентов по категориям и типам угроз основано на внутренней классификации и методологии самого Solar JSOC. Отчет является только информативным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы российского рынка. Команда Solar JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

Сводная статистика за отчетный период

- Всего за третий квартал 2016 года в Solar JSOC было зафиксировано **63 224 события** с подозрением на инцидент, в то время как за аналогичный период прошлого года их количество составило только 54 578, а в Q2 2016 – 68 823. Снижение на 8% по сравнению с Q2 2016 объясняется тем, что за третий квартал 2016 года были оптимизированы сценарии выявления инцидентов в ранее подключенных компаниях, основанные на профилировании сетевой и хостовой активностей.
- В третьем квартале 2016 года доля критичных инцидентов составила 14,3%, что ниже аналогичного показателя в **Q2 2016 года, равного 11,2%**. Это связано с общим снижением бизнес-активности подключенных компаний в начале года.
- Среднее время принятия инцидента в работу специалистом JSOC с момента выявления составило **18,7 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций по критичным инцидентам составило **24,3 минуты и 72,8 минуты** по всем остальным с момента возникновения инцидента.
- Соблюдение клиентских SLA за первый квартал 2016 года составило **97,8%**.
- **69,6%** исследованных событий зафиксировано при помощи основных сервисов ИТ-инфраструктуры и средств обеспечения базовой безопасности: межсетевые экраны и сетевое оборудование, VPN-шлюзы, контроллеры доменов, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, системы обнаружения вторжений).
- При этом стоит отметить, что оставшиеся инциденты **(30,4%),** выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и критичность для информационной и экономической безопасности компании-клиента, что позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные таргетированные атаки.

Классификация инцидентов по критичности

Основным критерием при классификации инцидентов по критичности является воздействие инцидента на ключевые бизнес-процессы и информационные ресурсы компании-клиента.

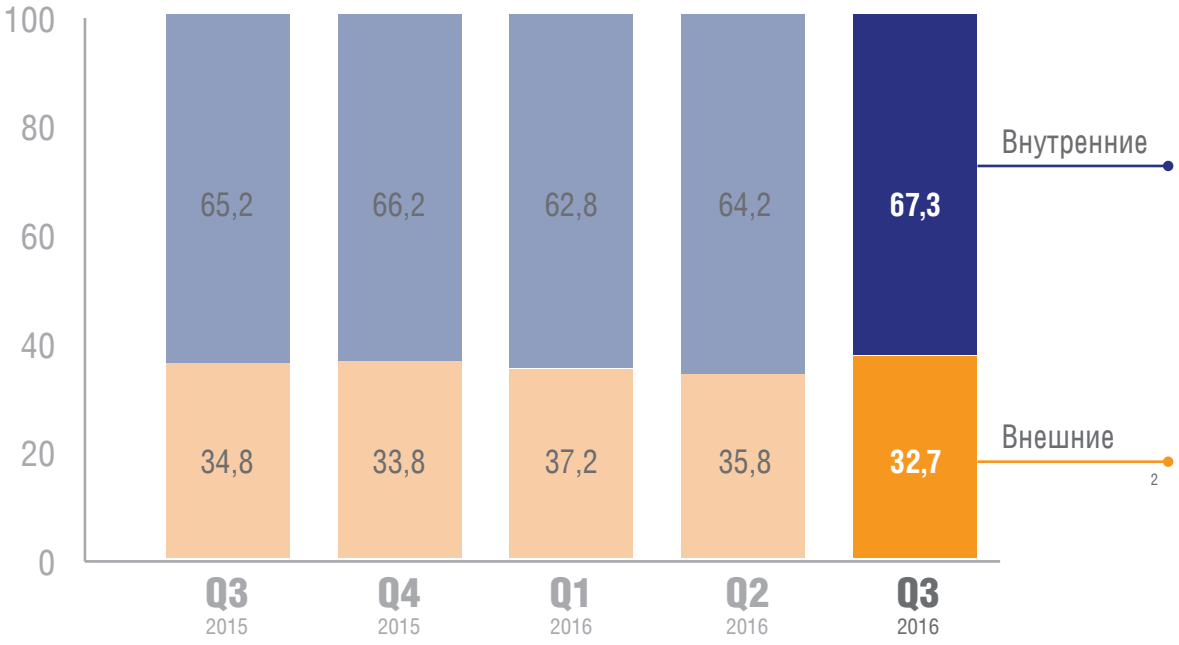
Инцидент считается критичным, если в результате него возможны и высоковероятны следующие события:

- длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical;
- повреждение, потеря или компрометация критичной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам;
- прямые финансовые потери на сумму более 1 млн рублей в результате действий внутренних сотрудников или киберпреступников.

Общие показатели по инцидентам

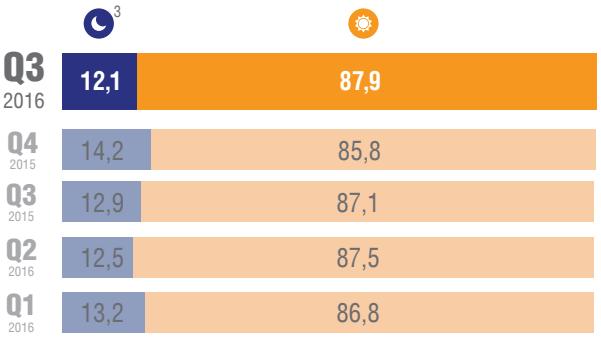
Q3 2016

Распределение инцидентов по внешним и внутренним

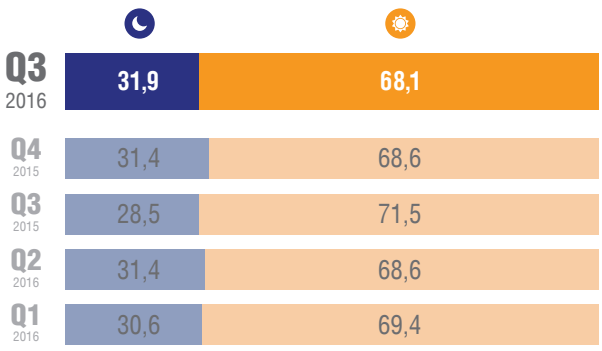


Распределение количества инцидентов по времени суток

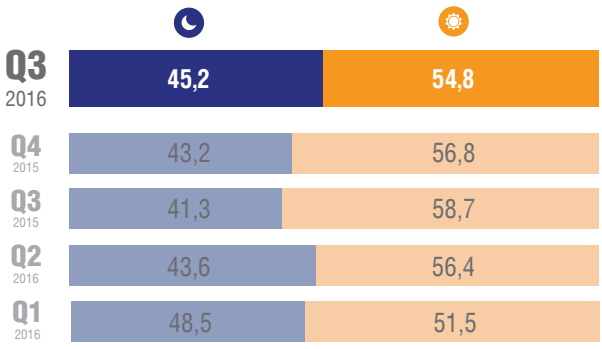
Время суток:



Распределение по критичным инцидентам:



Распределение по критичным внешним инцидентам:



Ночь
С 21:00 до 08:00 по времени расположения офиса заказчика

День
С 08:00 до 21:00 по времени расположения офиса заказчика

[2] К внутренним пользователям - инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты.

[3] С 21:00 до 08:00 утра по времени расположения офиса и присутствия специалистов информационной безопасности Заказчика.

Выводы по общим показателям по инцидентам

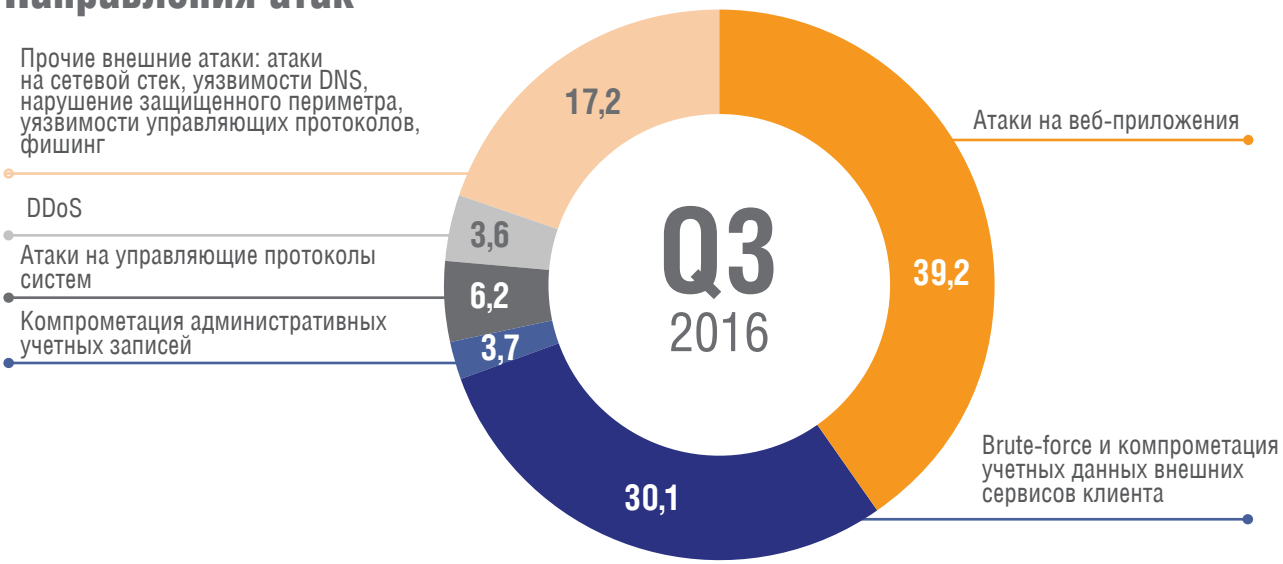
Анализ статистики внешних и внутренних инцидентов за 2015 и 2016 год позволяет выявить зависимость их распределения в течение года. Так, количество внутренних инцидентов имеет тенденцию к нарастанию от начала к концу года: в Q1 2016 их доля составляла 62,8%, а в Q3 2016 уже 67,3%. На основании этих выводов мы прогнозируем дальнейший рост доли внутренних инцидентов в Q4 2016 до отметки 68,3%.

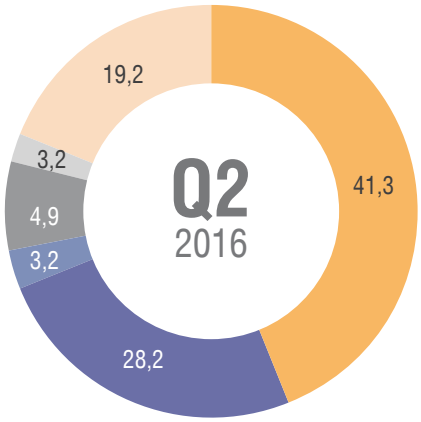
В Q3 2016 подтверждается тенденция роста доли ночных критичных инцидентов в течение года, что связано с уплотнением количества внутренних бизнес-задач, приходящихся на нерабочее время или выходные дни. При этом количество ночных критичных внешних инцидентов тоже выросло с 43,6% в Q2 2016 до 45,2% в Q3 2016.

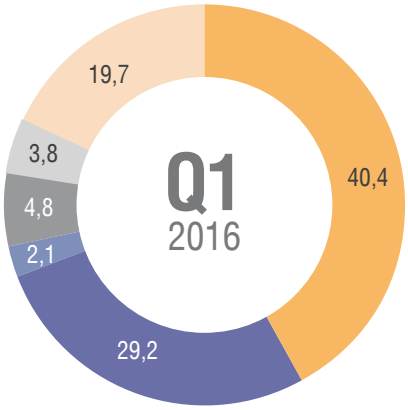
Внешние инциденты

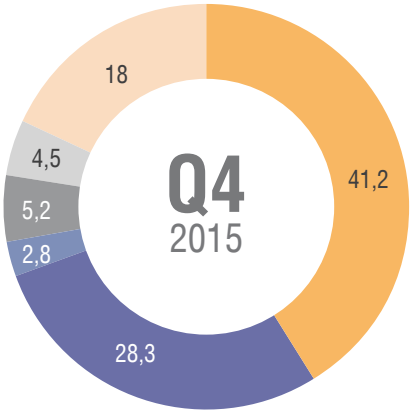
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся сотрудниками компании-клиента. «Простые атаки», а именно, действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не влекущие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей – из отчета исключены.

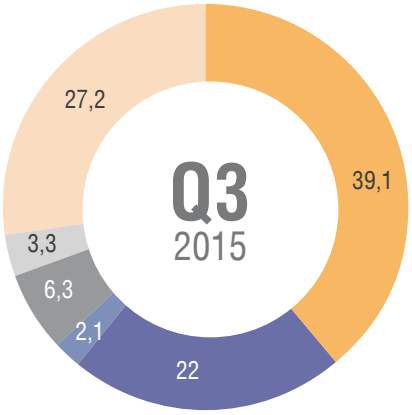
Направления атак











Особенности внешних инцидентов в третьем квартале 2016 г.:

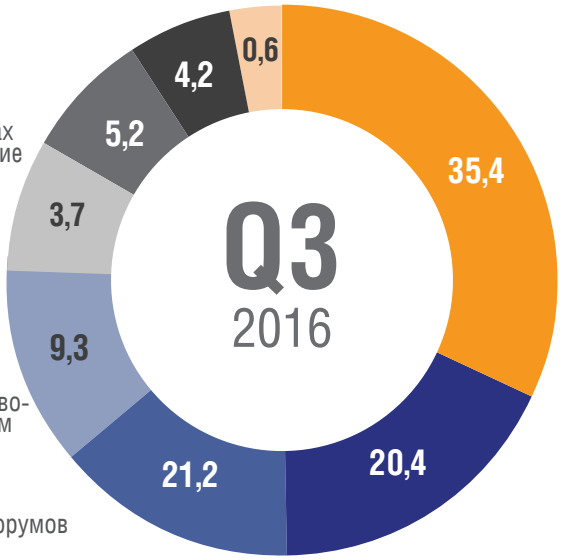
- В дополнение к ранее описанным трендам на атаки веб-приложений и компрометации клиентских учетных записей в Q3 2016 выявлены увеличения доли инцидентов, связанных с компрометацией административных учетных записей и атаками на управляющие протоколы. Так, в Q3 2016 было зарегистрировано 765 случаев компрометации административных учетных записей среди подключенных компаний-клиентов и порядка 1300 инцидентов, связанных с нарушениями использования управляющих протоколов систем и сервисов.
- Основываясь на тенденции роста числа DDoS-атак к концу года, мы прогнозируем рост их числа в Q4 2016 до 970 среди всех подключенных компаний-клиентов. Таким образом, в среднем в день в Solar JSOC будет регистрироваться более 10 DDoS-атак.
- Доля прочих внешних атак, таких как атаки на сетевой стек, эксплуатация уязвимостей DNS, организация фишинга и т.п. на протяжении первых трех кварталов 2016 года продолжает снижаться. Это говорит об упрощении векторов преодоления периметров компаний и стремлении внешних злоумышленников к эксплуатации известных уязвимостей подсистем аутентификации и авторизации систем и сервисов, а также внешних веб-приложений.

Внутренние инциденты

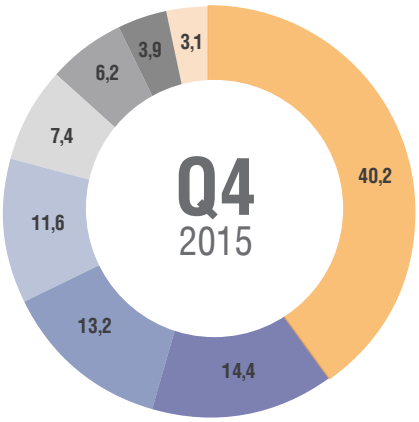
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников компаний-клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных данных сотрудников к внутренним системам, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем.

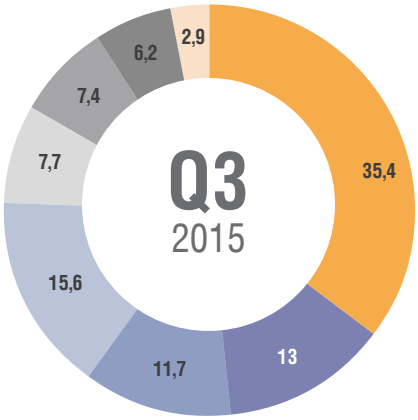
Направления атак

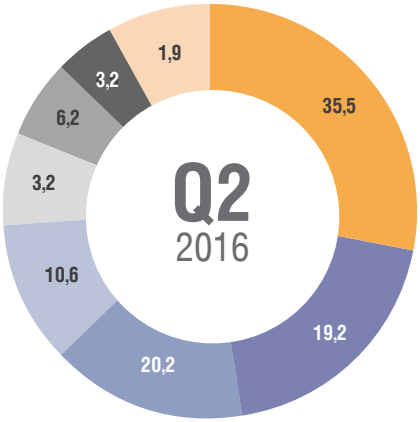
- Утечки конфиденциальных данных
- Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
- Нелегитимные работы под привилегированными учетными записями: внутренние пользователи
- Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критичных бизнес-систем
- Нарушение политик доступа в интернет, в том числе использование TOR-клиентов, анонимайзеров и посещение хакерских форумов

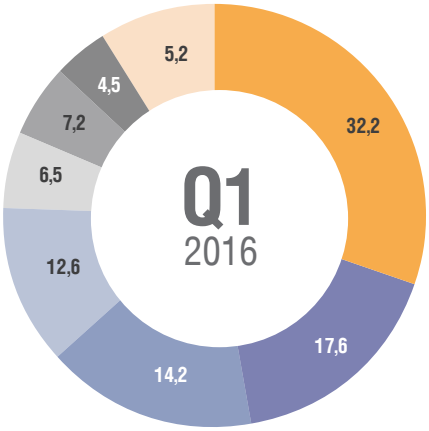


- Вирусные атаки, включая массовые вирусные заражения, действия ransomware и поведенческое выявление zero-day
- Прочее
- Компрометация внутренних учетных записей

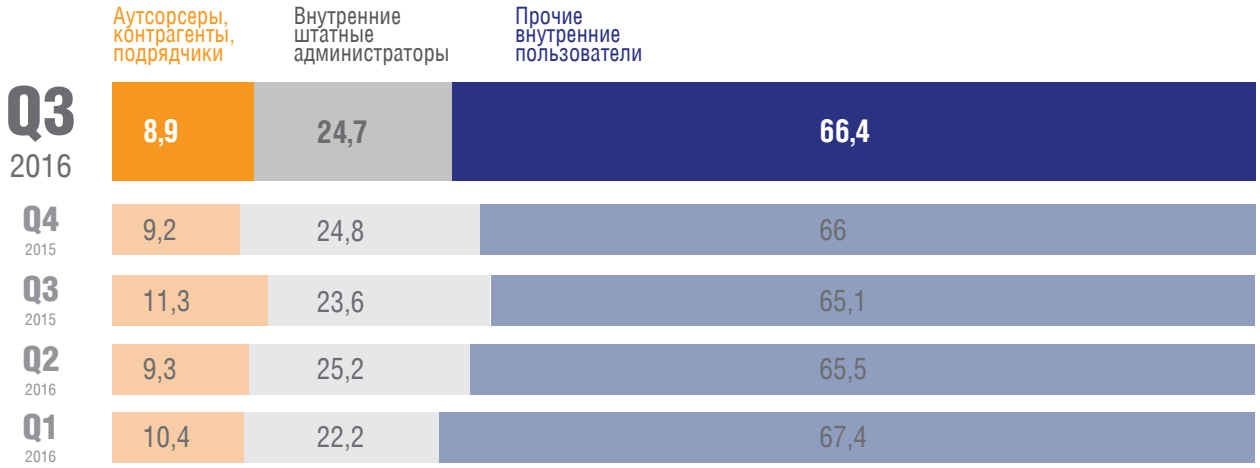




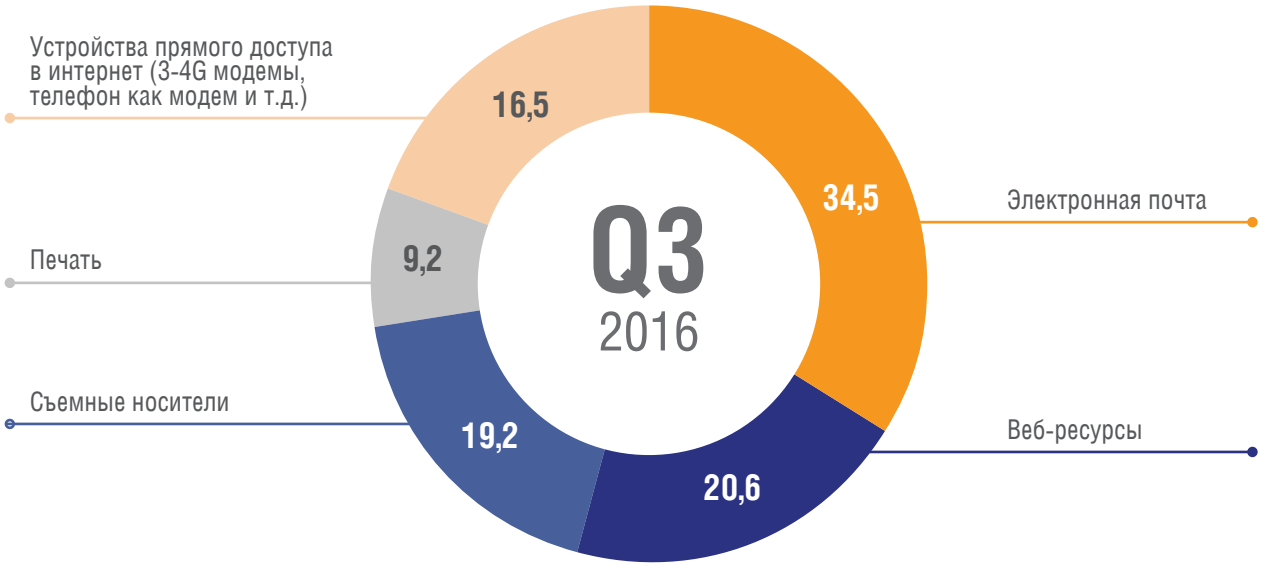


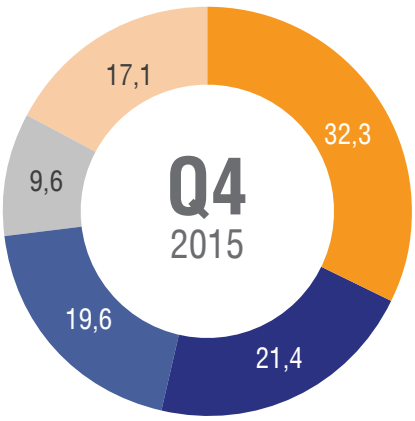


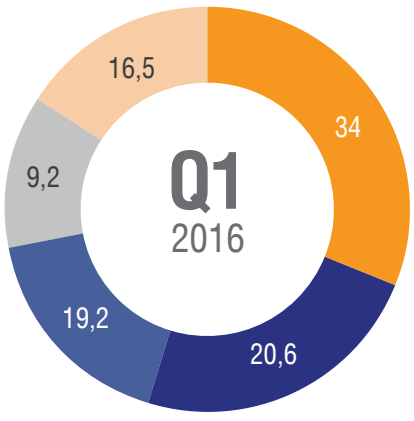
Инициаторы внутренних инцидентов

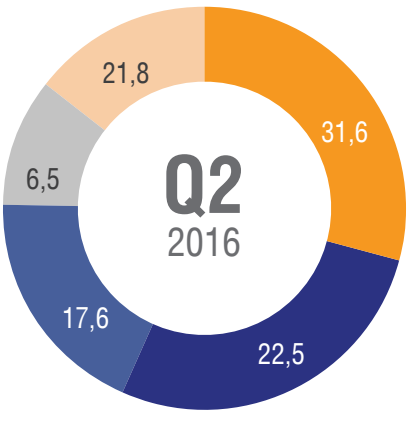


Распределение инцидентов по каналам утечек









Особенности внутренних инцидентов в третьем квартале 2016 г.:

- На протяжении последних четырех кварталов отмечается уверенный рост числа массовых заражений троянами, доставляемых посредством псевдополезного программного обеспечения (ransomware). Вместе с аналогичным ростом доли инцидентов, связанных с компрометацией внутренних учетных записей, можно сделать вывод, что эти два вектора связаны. Загруженный и активированный вирус/троян становится средством перехвата паролей с целью углубления разведки в инфраструктуре из-под легитимной учетной записи.

- На длительном периоде времени мы отмечаем снижение доли инцидентов, связанных с нарушениями политик доступа в Интернет, использования Tor-клиентов, посещения хакерских форумов и использования анонимайзеров, но при относительно высоком уровне числа подключений сторонних устройств доступа в Интернет (смартфоны в режиме Wi-Fi точки доступа, USB 3G/4G-модемы) мы предполагаем, что данная нелегитимная активность сохраняется и для ее мониторинга и контроля требуется подключение большего числа рабочих станций на уровне локальных логов.

Результаты использования информации об угрозах от FinCERT

За третий квартал 2016 командой Solar JSOC был получен 41 информационный бюллетень от FinCERT, содержащий технические данные о зарегистрированных атаках, используемом способе проникновения и вредоносном коде, различными сетевыми и хостовыми индикаторами компрометации систем. Информация из каждого бюллетеня в течение 3 часов заносится в системы контроля защищенности и мониторинга инцидентов для проведения проверки и выявления подозрительных хостов в инфраструктуре подключенных компаний-клиентов.

По результатам отработки информационных бюллетеней FinCERT в Q3 2016 командой Solar JSOC была собрана следующая статистика:

- Признаки наличия сетевых индикаторов обнаружены по 20 бюллетеням в 31 подключенных компаниях (одни бюллетени встречались в нескольких компаниях), причем 11 случаев были определены как подтвержденные инциденты с проведенными дальнейшими расследованиями

- Признаки наличия хостовых индикаторов обнаружены по 15 бюллетеням в 26 подключенных компаниях, причем только 3 случая определены как ложные срабатывания

Из выявленных и подтвержденных инцидентов в 7 случаях оперативное взаимодействие команды Solar JSOC с клиентом позволило существенно минимизировать ущерб. Во всех остальных случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от возникшего инцидента.